UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/788,999	02/26/2004	Michael W. Brown	AUS920031034US1	9234

46240 7590 11/17/2008

IBM CORPORATION (WMA)
C/O WILLIAMS, MORGAN & AMERSON, P.C.
10333 RICHMOND, SUITE 1100
HOUSTON, TX 77042

EXAMINER	
GUPTA, MUKTESH G	

ART UNIT	PAPER NUMBER
2444	

MAIL DATE	DELIVERY MODE
11/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/788,999	BROWN ET AL.	
	Examiner	Art Unit	
	Muktesh G. Gupta	2444	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16 and 34-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16 and 34-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/27/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

LDETAILED ACTION

1. Amendments received on 08/29/2008 have been entered.

Claims 1-3, 9-11 and 14-16 are amended.

Claims 17-33 are cancelled.

Claims 1-16, 34-38 have been examined on merits and are pending in this application.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/29/2008 has been entered.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 10/27/2008 is being considered by the examiner.

Response to Arguments

4. Applicant's arguments with respect to pending claims have been considered but are moot in view of the new ground(s) of rejection.

a. Applicant's arguments with respect to **Claim 1** have been considered but are moot in view of the new ground(s) of rejection.

b. Applicant's arguments and amendments filed on 08/29/2008 have been carefully considered but they are deemed moot in view of the following new grounds of rejection as explained here below, necessitated by Applicant's substantial amendment to the claims "reducing the electronic mail message by removing the unauthorized portion but retaining at least a portion of the electronic mail message that the user is authorized to receive", which significantly affected the scope thereof.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-16, 34-38** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Application Publication No. 20050038750 to Cahill et al., (hereinafter "Cahill"), as applied to **Claims 1-16, 34-38** and further in view of US Patent Application Publication No. 20020059425 to Belfiore, Joseph et al., (herein after "Belfiore").

a. Regarding **Claims 1-16, 34-38** Cahill discloses substantially the invention as claimed. Cahill does not explicitly disclose or clear about reducing the electronic mail message by removing the unauthorized portion.

b. Cahill discloses (as stated in par. 0041, par. 0075, par. 0078-0090, par. 0077, FIG. 1 and the following discussion are intended to provide a brief general description of a suitable computing environment in which the invention may be implemented. It should be understood, however, that handheld, portable, and other computing devices of all kinds are contemplated for use in connection with the present invention. While a general purpose computer is described below, this is but one example, and the present invention requires only a thin client having network server interoperability. and interaction. Individual inside or outside the organization that receives such an rights management email and the content 32 therein cannot render such content 32 if such individual cannot obtain a license 36 corresponding to the email content 32, or if the rules and requirements of the obtained license 36 do not in fact allow the individual to so render. Significantly, inasmuch as the email with the protected content 32 may be received by an (Rights Management) RM-compliant individual with a trusted component 38 and the like, such email should be in a form amenable to such RM-compliant individual. At the same time, inasmuch as the email with the protected content 32 may be received by a non-RM-compliant individual without a trusted component 38 and the like, such email should also be in a form amenable to such non-RM-compliant individual, at least to the extent that the email is recognizable as such

by the computing device of the non-RM-compliant individual, informs the non-compliant individual of the protected content 32 therein and does not inappropriately affect the computing device of the non-RM-compliant individual. The structure of an RM-protected email message is consistent with a MIME or MAPI representation of an email message with an attachment. Further, in such embodiment, the attachment includes protected content 32 of the email along with other RM-related information. Generalized MIME or MAPI structure for an email is set forth: HEADER, MAIN INFO, AS PLAIN TEXT, AS HTML, AS OTHER, ATTACHMENT(S). The HEADER portion contains basic information relating to the email, including a date, any subject information, the sender, the recipient, and/or the like. The MAIN INFO portion contains the body of the email, which may include text, pictures, links, and/or the like. Notably, inasmuch as some recipients may have different email capabilities, the MAIN INFO portion can include several alternative versions of the body of the email, including the body AS PLAIN TEXT for a recipient that cannot handle anything more complex than plain text, and the body AS HTML for a recipient that can handle more complex HTML (Hyper Text Markup Language) formatting. Of course, other alternative versions of the body may also be included, such as for example a version with the body in an XML (eXtensible Markup Language) format. The ATTACHMENT portion can contain most any information that a sender wishes to attach to an email, such as for example one or more files, or one or more other pieces of information to be included with the email. The main info 48 of the email

44 may contain a message to the effect that the email 44 is RM-protected and therefore not viewable by the non-RM-compliant individual. Alternatively, the main info 48 of the email 44 may have another message, an advertisement, a link for more information on RM-compliant email 44, etc. the license 36 for the email protected content 32 is typically obtained from an RM server 54 (FIG. 3) operated by or on behalf of the organization. Such license 36 may be sent with the email under at least some circumstances, may be obtained upon opening the email, may be obtained upon downloading the email, may be obtained at the direction of the recipient, and/or the like. Moreover, such obtaining may be performed manually or automatically if circumstances allow. In examining the attachment 44 of the email 46 certain identifying indicia may be found. Rights data 50 may be defined by the sender of the email or custom rights data or rights data as obtained from a pre-defined template, may be defined by a template selected by the sender of the email, and sets forth each individual or group of individuals that has rights with respect to the protected content 32, and for each such individual or group of individuals a description of such rights. Cahill does display in Figure 5, Not RM-enabled and RM-enabled clients can both open the e-mail, Main info of email is only displayed to Not RM-enabled client, indicating that the e-mail is RM protected and the information how to procure the protected content of the identified attachments. While in case of RM-enabled client, can open the e-mail, recognize protected content and protected content 32 in the attachment is displayed upon the approval of the trusted component 38 and

decryption of such protected content 32 for rendering protected content in attachment. The protected content than can be downloaded from the server after fulfilling the license requirement. Thus it is clear that Cahill does teach that both Not RM-enabled and RM-enabled clients are getting different version of the e-mail using different templates, which can be displayed on any thin client device or computing device, with scaling back size for the thin client device, Though it does not explicitly disclose the same.

c. Belfiore does disclose (as stated in par. 0205-0207, par. 0213, par. 0090-0099, par. 0143-0145, par. 0153, Referring to FIG. 10, security component 165 includes an authorization module 1104. Authorization module 1104 includes various hardware and/or software modules and components to determine what actions an authenticated entity may perform in a dynamic environment in which group membership, roles and delegation of rights of each entity may be changed. Authorization module 1104, in combination with other modules of security component 165, accomplishes advancement in the authorization field and technology is through digital rights management. Digital Rights Management (DRM) involves the automated enforcement of rules and conditions on the use and distribution of information and content. At the heart of DRM is a premise that runs against traditional system security intuition. In typical system security, the source of authority to access data or information is a user. Once a user is authenticated, access to services is authorized based on user identity. As such, software is authorized to the extent rights are granted to the underlying user. The

rights of the owner (and the permissions granted to the user) are named in a standard language. The rights are enforced by a "device," such as but not limited to various hardware and/or software modules and components, that insures that only trusted software, software that has previously been authenticated and obligated to enforce the rights and limitations specified by the owner, is granted access to the information. This allows a content owner to delegate rights, not to a user, but to a piece of software that will restrict access to content based on the terms defined by the owner. Security component 165 is distributed throughout the server federation 120 and thereby provides distributed network security. Generally, the distributed nature of security component 165 provides end-to-end confidentiality and integrity of message content, whether host-to-host or point-to-point, while permitting intermediate proxy servers to route events and messages correctly. The user interface component 140 of the platform 115 of FIG. 1 provides a multi-modal, responsive, and intelligent user interface across a variety of client devices. FIG. 4 schematically illustrates the user interface component 140. The user interface component 140 provides a multi-modal user interface (UI), meaning that the user can interact with the UI through multiple modes and the modes can be seamlessly changed on-the-fly. The user interface component 140 includes an advanced input/output component 400 to allow multi-modal input and output. In addition to being multi-modal, the user interface component 140 is responsive in that it adapts and/or changes based on the user's state and context across a number of client devices 110. For example, the user interface will be

configured and rendered according to the user's preferences and session status so that if the user switches mid-session from one client device to another, the user may continue the session using the other client device with the user interface appearing consistent (although possibly modified, as discussed below) across client devices. The user interface also scales appropriately and smoothly to the technical capabilities of the client device. For example, mobile telephones have obvious technical limitations in their user interface due to space limitations for input keys and display area. The user interface for these mobile telephones would be scaled down so as to emphasize only the more important features of the user interface. The messaging component 160 of the invention enables client devices 110 and servers 140 to communicate. The term "message" extends to structured data exchanged between applications or other components of the operating environment 100. Examples of messaging include application-to-application messaging, person-to-person messaging (email) and collaborative applications. In order to facilitate interoperability, the messaging component 160 provides a common messaging application program interface (API) and set of services that layer on top of HTTP, SMTP and/or other transports to provide common semantics to messaging applications regardless of the underlying transport. Moreover, the messaging component 160 is highly scalable both in number of users and connected devices that it can support, and also in the types of devices or networks with which it can be used. In other words, the messaging component 160 readily adapts for use with devices and systems ranging from

small wireless devices to "mega-scale" networks and messaging systems. This scalability feature is characterized by the ability to build messaging applications on the messaging platform that allow small devices to participate in high quality of service (QOS) message exchanges as well as sophisticated distributed services. In other words, the messaging component 160 is both highly scalable on the server and can be scaled down to small devices, meaning that it is possible to build appropriate "small footprint" subsets. The security services of layer 702 can enable authentication, access control and/or secrecy services according to the security component 165. For example, authentication may be based on certificates according to an end-to-end model, which can be user-based or machine-based, or can be provided according to other models, including XMLDSIG, MSMQ, Secure Multipurpose Internet Mail Extensions (S/MIME), or other suitable authentication systems. Access control (i.e., who is allowed to deliver to and manipulate queues) may be controlled in a user-oriented fashion based on credentials established in message authentication. Secrecy services (i.e., encryption and decryption) may be established using hop-to-hop secrecy enabled through HTTPS, which implies that intermediate servers are trusted. End-to-end secrecy can be enabled though key exchange protocol.

d. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Cahill's rights management implemented protected content delivery system which through the trust-based RM system which allows an owner of digital content to specify license rules that must be satisfied before

such digital content is allowed to be rendered on a user's computing device, and current real-time situation including "who, where, and when" awareness, to Belfiore's system, in which depending on the user interface capabilities of the client, the page component (content) may silently redirect invocations to particular versions of the page (content) that are compatible with the client, device. Regardless of the page(content) version, however, the user interface will appear consistent across a wide range of client devices, though some features will be present or more fully developed in richer versions of the page (content).

e. The motivation would have been for an effective and particularly for a way to more efficiently utilize various communication protocols, resources, to implement Rights management, RM enforcement to allow the controlled rendering of forms of digital content, where such control is flexible and definable by the content owner of such digital content, and device capabilities of the recipients', mobile terminal having limited processing capabilities to receive content based on rights management as well type of device, where content is scaled back.

f. Therefore, it would have been obvious to combine these two references of Cahill's and Belfiore's disclosures in light of providing system, method and program which efficiently integrates multiple profiles, matches profiles, services, optimizes, coordinates and processes at the back end to, provide unified and interactive Access Point pushing information to the terminal where the pushed

information matches the content and services based on rights management and capabilities of recipients type of device.

Together Cahill and Belfior disclosed all limitations of ***Claims 1-16, 34-38*** *and hence are rejected under 35 U.S.C. 103(a).*

As to Claim 1 *Cahill anticipates method, comprising:*

determining that a user is authorized to receive less than all of an electronic mail message based on at least one digital fight associated with the electronic mail message (as stated in par.0189, lines 1-18, Rights management (RM) enforcement architecture and method allow the controlled rendering of arbitrary forms of digital content (including electronic mail message), where such control is flexible and definable by the content owner/developer of digital content. Controlled rendering, where digital content are to be shared amongst a defined group of individuals or classes of individuals is achieved through Rights-managed email, propagating RM protection to attachments of RM-protected email, dynamic application of RM protection to a document in a document store, RM-protected email conversations);

reducing the electronic mail message by removing the unauthorized portion but retaining at least a portion of the electronic mail message that the user is authorized to receive (as stated in par. 0079-0090, par. 0099, lines 6-19, par. 0089, lines 12-22, par. 0091, lines 1-22, structure of an RM-protected email message is consistent with a MIME or MAPI representation of an email message with an attachment. Further, in such embodiment, the attachment includes protected content 32 of the email along with other

RM-related information. The ATTACHMENT portion can contain most any information that a sender wishes to attach to an email, such as for example one or more files, or one or more other pieces of information to be included with the email. In the latter category, such other piece of information may for example include specific information that the sender wishes to send to the recipient but that does not fit elsewhere within the email. In particular, and as seen in FIG. 4, in the embodiment, the email 44 contains the protected content 32 as being embedded within an attachment 46 to the email 44, and the trusted component 38 and the email application on the computing device 34 of an RM-compliant individual are aware that such protected content 32 is in the attachment 46. Of course, such protected content 32 in the attachment 46 is of no use to a non-RM-compliant individual and an email application thereof at a computing device thereof, and accordingly the main info 48 of the email 44 may contain a message to the effect that the email 44 is RM-protected and therefore not viewable by the non-RM-compliant individual. Alternatively, the main info 48 of the email 44 may have another message, an advertisement, a link for more information on RM-compliant email 44, etc., it may be the case that the message in the main info 48 of the email 44 is bypassed entirely and is not displayed to the RM-compliant individual. Instead, the protected content 32 in the attachment is displayed upon the approval of the trusted component 38 and decryption of such protected content 32. turning now to FIG. 6, the rights data 50 in the attachment 46 of the email 44 is retrieved and forwarded to the RM server 54 (step 601), and such RM server 54 determines that the RM-compliant recipient is one of the individuals or in one of the groups of individuals listed in the rights data 50 (step 603) and thereafter

issues a license 36 corresponding to the protected content 32 to the recipient based on the rights data 50 (step 605), where such license 36 specifies the rights the recipient or what the recipients are authorized with respect to the protected content 32 as determined from the rights data 50, and also includes from the rights data 50 a decryption key (KD) for decrypting the encrypted content 32. As was set forth above, such (KD) may be encrypted in a manner decryptable by the trusted component 38 of the computing device 34 of the recipient. It may be the case that the message in the main info 48 of the email 44 is by passed or removed entirely and is not displayed to the RM-compliant individual and the protected content 32 in the attachment is displayed upon the approval of the trusted component 38 and decryption of such protected content 32. Such decryption key (KD) by itself be encrypted to prevent unauthorized use thereof. Accordingly, the decryption key (KD) in the rights data 50 is encrypted according to a public key of the aforementioned RM server 54 (PU-RM) operated by or on behalf of the organization to result in (PU-RM(KD));

and providing the reduced electronic mail message to the user (as stated in par 0096, lines 1-5, par. 100, email created (selected) by a sender as set forth herein and sent to authorized recipient. the protected/encrypted content 32 of the email 44 is compressed to reduce the overall size thereof. The trusted component 38 may decompress the encrypted and compressed content 32 in the course of decrypting same. The trusted component 38 of the computing device 34 of the RM-compliant recipient then reviews the issued license 36 to determine that the recipient has the right to view the content 32 (step 607), and thereafter retrieves (KD) from the license 36 and

the protected content 32 from the email 44 (step 609), decrypts the protected content 32 with (KD) (step 611), and presents the decrypted content 32 for rendering (step 613). Note that based on the rights the recipient has with respect to the content 32 as set forth in the license 36, the trusted component 38 may take other appropriate actions. For example, if the recipient does not have the right to copy or print the content 32, the trusted component 38 would direct the email application to turn off such functions with respect to such content 32).

As to Claim 2, *Cahill anticipates method of claim 1, wherein determining that the user is authorized to receive less than all of the electronic mail message comprises determining that the user is authorized to receive less than all of the electronic mail message based upon at least one of a copyright, a distribution right, a broadcast right, a reproduction right, a publication right, a licensing restriction, fair use, and a restriction imposed by the Digital Rights Millennium Copyright Act (as stated in par. 0011, lines 1-5, par. 0012, lines 1-5 and par 0013 lines 1-5, Digital rights management and enforcement is implemented with Rights management in connection with digital content such as digital audio, digital video, digital text, digital data, digital multimedia, etc., where such digital content is to be distributed to one or more users, or digital content owner or rights-owner such as an author, a publisher, a broadcaster, etc., wishes to distribute such digital content to each of many users or recipients in exchange for a license fee while at the same time holding the user to the terms of type of license. Digital rights management gives the owner, choice to restrict what the users can do*

with such distributed digital content beyond there authorization and terms of type of license).

As to Claim 3, *Cahill anticipates method of claim 1, wherein determining that the user is authorized to receive less than all of the electronic mail message comprises accessing at least one of a user input and a user profile further comprising (as stated in par. 0048, lines 1-23, par. 0050, lines 1-14 and par. 0051, lines 1-18, par. 0064-0067, User enter commands and information (for stored user-profiles and login ID) into the computer through input devices connected to the processing unit through a user input interface that is coupled to the system bus connected by other interfaces, such as a parallel port, game port, universal serial bus, display device, network interface to establishing communications over the WAN, such as the Internet to servers and other computers and for accessing electronic mail messages from the mail-servers. Referring to FIG. 3, rights management (RM) and enforcement is highly desirable in connection with digital content 32 such as digital audio, digital video, digital text, digital data, digital multimedia, etc., where such digital content 32 is to be distributed to users. Typically, a content owner or developer distributing such digital content 32 wishes to restrict what the user can do with such distributed digital content 32. An RM system 30, then, allows the controlled rendering of arbitrary forms of digital content 32, where such control is flexible and definable by the content owner of such digital content. Typically, content 32 is distributed to the user in the form of a package 33 by way of any appropriate distribution channel. The digital content package 33 as distributed may include the*

digital content 32 encrypted with a symmetric encryption/decryption key (KD), (i.e., (KD(CONTENT))), as well as other information identifying the content, how to acquire a license for such content, etc.):

providing to the user information relating to at least one portion of content of the electronic mail message (as stated in par. 0086, HEADER portion contains basic information relating to the email, including a date, any subject information, the sender, the recipient, and/or the like. The MAIN INFO portion contains the body of the email, which may include text, pictures, links, and/or the like. Notably, inasmuch as some recipients may have different email capabilities, the MAIN INFO portion can include several alternative versions of the body of the email, including the body AS PLAIN TEXT for a recipient that cannot handle anything more complex than plain text, and the body AS HTML for a recipient that can handle more complex HTML (Hyper Text Markup Language) formatting. Of course, other alternative versions of the body may also be included, such as for example a version with the body in an XML (eXtensible Markup Language) format);

providing to the user information relating to the unauthorized portion, wherein the unauthorized portion is associated with at least one protected content indicator (as stated in par. 0089, accordingly the main info 48 of the email 44 may contain a message to the effect that the email 44 is RM-protected and therefore not viewable by the non-RM-compliant individual. Alternatively, the main info 48 of the email 44 may have another message, an advertisement, a link for more information on RM-compliant email 44, etc., i.e. content 32 of the email can only be rendered by a recipient that can obtain

a license 36 for the content 32, where the license 36 allows such recipient to in fact render the content 32 of the email);

receiving, from the user, at least one preference for reducing the electronic mail message (as stated in par. 0069-0073, par. 0093-0094, the digital content 32 will not be rendered unless the rules and requirements within the license 36 are satisfied. Preferably, then, the user's computing device 34 is provided with a trusted component or mechanism 38 that will not render the digital content 32 except according to the license rules embodied in the license 36 associated with the digital content 32 and obtained by the user. The rules and requirements in the license 36 can specify whether the user has rights to render the digital content 32 based on any of several factors, including who the user is, where the user is located, what type of computing device the user is using, what rendering application is calling the RM system, the date, the time, etc. In addition, the rules and requirements of the license 36 may limit the license 36 to a pre-determined number of renderings, or pre-determined rendering time, for example. The rules and requirements may be specified in the license 36 according to any appropriate language and syntax. For example, the language may simply specify attributes and values that must be satisfied, or may require the performance of functions according to a specified script. Still referring to FIG. 4, it is seen that the protected content 32 in the attachment 46 of the email 44 may actually comprise several alternative forms of the body of the email 44, which again may include text, pictures, links, and/or the like. As before, the alternative forms may be provided inasmuch as some recipients may have different email capabilities. such protected content

attachments 52 may be organized in any particular manner. For example, in one scenario, the attachments 52 may be organized into a list that also includes as a preface or the like the number of attachments 52 and the name of each attachment 52, and includes as a postscript or the like metadata relating to the addenda, if any);

and wherein reducing comprises reducing based upon the preference received from the user, wherein the preference refers to a reduced resolution version of the electronic email message and a transfer criteria associated with downloading of the electronic mail message (as stated in par. 0130, par. 0152, the license 36 for the document content 32 is typically obtained from an RM server 54 (FIG. 3) operated by or on behalf of the organization. Further, in such embodiment, the custom data section includes protected content 32 of the document along with other RM-related information. The generalized RM-protected document structure is set forth: DOCUMENT PROPERTIES, CUSTOM PROPERTIES, STORAGE, And CUSTOM DATA. The custom data 66 has another section 64 with transforms 70 that specify to a document application 56 or the like how to get at the protected content 32. In particular, such transforms 70 may have a RM part specifying each section 64 of custom data 66 that is encrypted and each section 64 of custom data with a license 36 by which a decryption key (KD) may be obtained. In addition, such transforms 70 may have a compression part specifying each section 64 of custom data 66 that is compressed and how the section is compressed. Of course, the transforms 70 may have other parts with other accessing information);

wherein providing the reduced electronic mail message includes providing using trickle downloading (as stated in par. 0077, Such license 36 may be sent with the email under at least some circumstances, may be obtained upon opening the email, may be obtained upon downloading the email, may be obtained at the direction of the recipient, and/or the like. Moreover, such obtaining may be performed manually or automatically if circumstances allow);

and wherein the reduced electronic mail message includes an attachment, wherein the digital right is associated with the attachment, and wherein providing the reduced electronic mail message includes providing less than all of the attachment based on the associated digital right (as stated in par. 0079, par. 0089-0095, the structure of an RM-protected email message is consistent with a MIME or MAPI representation of an email message with an attachment. Further, in such embodiment, the attachment includes protected content 32 of the email along with other RM-related information. The trusted component 38 and the email application on the computing device 34 of an RM-compliant individual may become aware that the protected content 32 is in the attachment in any appropriate manner. For example, in examining the attachment 44 of the email 46 certain identifying indicia may be found, and as also seen in FIG. 4, the attachment 46 of the email 44 with the protected content 32 is organized in the following manner. In general, the attachment 46 has the protected content 32 and also has rights data 50 relating to the protected content 32. As may be appreciated, the rights data 50 may be defined by the sender of the email or may be defined by a template selected by the sender of the email, and sets forth each individual or group of

individuals that has rights with respect to the protected content 32, and for each such individual or group of individuals a description of such rights. Still referring to FIG. 4, it is seen that the protected content 32 in the attachment 46 of the email 44 may actually comprise several alternative forms of the body of the email 44, which again may include text, pictures, links, and/or the like. As before, the alternative forms may be provided inasmuch as some recipients may have different email capabilities. For example, in one scenario, the attachments 52 may be organized into a list that also includes as a preface or the like the number of attachments 52 and the name of each attachment 52, and includes as a postscript or the like metadata relating to the addenda, if any. the protected/encrypted content 32 of the email 44 is compressed to reduce the overall size thereof. As may be appreciated, the trusted component 38 may decompress the encrypted and compressed content 32 in the course of decrypting same. As may also be appreciated, such compression provides a significant reduction in the overall size of the email 44 having the protected content 32 in the attachment 46 thereof).

As to Claim 4, *Cahill anticipates method of claim 3, wherein accessing the user profile comprises accessing the user profile on at least one of a local device and a remote device (as stated in par. 0050, lines 1-14 and par. 0053, lines 1-11, computers operate in a networked environment using logical connections to one or more remote computers. The remote computer may be a personal computer, a server, a mail-server, a router, a network PC, a peer device or other common network node, and includes many or all of the elements described above relative to the computer. User-profiles are*

stored on both the computer and remote servers, which implicate authentication techniques for trusted electronic mail message exchange).

As to Claim 5, *Cahill anticipates method of claim 1, further comprising acquiring authorization to receive a protected portion of the electronic mail message (as stated in par. 0090, lines 1-20, e-mail attachment has protected content and also has rights data (means for authorization) relating to the protected content defined by the sender of the email or may be defined by a template selected by the sender of the email, and sets forth each individual or group of individuals that has rights with respect to the protected content, and for each such individual or group of individuals a description of such rights (means for authorization)).*

As to Claim 6, *Cahill anticipates method of claim 5, wherein acquiring the authorization comprises acquiring a license to receive the protected portion of the electronic mail message (as stated in par. 0067, lines 1-12, rights management system, allows the controlled rendering of arbitrary forms of digital content, where such control is flexible and definable by the content owner of such digital content (protected content). Content is distributed to the user in the form of a package by way of any appropriate distribution channel (through electronic mail message). The digital content package as distributed includes the digital content encrypted with a symmetric encryption/decryption key, as well as other information identifying the content, how to acquire a license for such content).*

As to Claim 7, *Cahill anticipates method of claim 5, wherein acquiring the authorization comprises directing the user to an owner of the digital rights to the protected portion of the electronic mail message (as stated in par. 0067, lines 1-12, rights management system, allows the controlled rendering of arbitrary forms of digital content, where such control is flexible and definable by the content owner of such digital content (protected content). Content is distributed to the user in the form of a package by way of any appropriate distribution channel (through electronic mail message). The digital content package as distributed includes the digital content encrypted with a symmetric encryption/decryption key, as well as other information identifying the content, how to acquire a license for such content and directing to owner for obtaining authorization for digital content (protected content)).*

As to Claim 8, *Cahill anticipates method of claim 1, further comprising providing the protected portion of the electronic mail message in response to acquiring the authorization (as stated in par. 0089, lines 11-19, protected content in the attachment RM-compliant individual and an email application thereof at a computing device, and accordingly the main info of the email contains a message to the effect that the email is RM-protected and therefore after authorization, have access to such protected content. Protected content in the attachment is displayed upon the approval (authorization) of the trusted component and decryption of such protected content).*

As to Claim 9, *Cahill anticipates method of claim 1, further comprising determining a format associated with the electronic mail message in response to determining that the user is authorized to receive less than all of the electronic mail message (as stated in par. 0065, lines 1-9, par. 0067, lines 3-8, and par. 0142, lines 1-3, RM system, allows the controlled rendering of multiple forms of digital content as digital audio, digital video, digital text, digital data, digital multimedia, etc., where digital content is to be distributed to users, control is flexible and definable by the content owner of such digital content. The main info of the email contains a message to that effect in the email, content is distributed to the user in the form of a package defining the selected format with all necessary RM-related information, RM-protected document with a custom data section, standard form of the protected content storage, etc. The protected content in the custom data may be in any particular format, which is selected);*

and wherein reducing the electronic mail message comprises reducing based on at least the determined format and wherein reducing comprises determining a format of at least one file associated with the electronic mail message(as stated in par. 0087, par. 0093-0095, The ATTACHMENT portion can contain most any information that a sender wishes to attach to an email, such as for example one or more files, or one or more other pieces of information to be included with the email. In the latter category, such other piece of information may for example include specific information that the sender wishes to send to the recipient but that does not fit elsewhere within the email. Still referring to FIG. 4, it is seen that the protected content 32 in the attachment 46 of the email 44 may actually comprise several alternative forms of the body of the email 44,

which again may include text, pictures, links, and/or the like. As before, the alternative forms may be provided inasmuch as some recipients may have different email capabilities. As shown, some of the alternative forms may include the body in plain text, in HTML, in XML, in rich text format (RTF), in plain text as HTML, etc. Of course, other alternative versions of the body may also be included in the protected content 32. Note that the protected content 32 may also include body information, such as for example whether the body is included in plain text or in HTML, and other body information. the protected content 32 may also include attachments to the body of the email 44, which inasmuch as the body of the email 44 is itself part of the attachment 46, will hereinafter be referred to as protected content attachments 52. As may be appreciated, such protected content attachments 52 may be organized in any particular manner. For example, in one scenario, the attachments 52 may be organized into a list that also includes as a preface or the like the number of attachments 52 and the name of each attachment 52, and includes as a postscript or the like metadata relating to the addenda, if any. the protected/encrypted content 32 of the email 44 is compressed to reduce the overall size thereof. As may be appreciated, the trusted component 38 may decompress the encrypted and compressed content 32 in the course of decrypting same. As may also be appreciated, such compression provides a significant reduction in the overall size of the email 44 having the protected content 32 in the attachment 46 thereof. Notably, such compression is not presently found by default in existing email formats).

As to Claim 10, *Cahill anticipates method of claim 9, wherein reducing the portion of the electronic mail message comprises identifying at least one chart, table, page, agenda, table of contents, summary, audio clip, or video clip based upon the determined file format (as stated in par. 0065, lines 1-9, par. 0067, lines 3-8, and par. 0142, lines 1-3, par. 0137, RM system, allows the controlled rendering of multiple forms of digital content as digital audio, digital video, digital text, digital data, digital multimedia, etc., where digital content is to be distributed to users, control is flexible and definable by the content owner of such digital content. The main info of the email contains a message to that effect in the email, content is distributed to the user in the form of a package defining the selected format with all necessary RM-related information RM-protected documents with a custom data section, standard form of the protected content storage, etc. The protected content in the custom data may be in any particular selected format. The DOCUMENT PROPERTIES portion contains basic information relating to the document, perhaps including an author, a creation date, and other parameters by which the document can be indexed. The CUSTOM PROPERTIES portion contains properties information that is not especially of interest to a user or the like and is not especially useful for indexing purposes but may be of use to another application. For example, such custom properties information may comprise content tagged according to an XML format for use by another application. The STORAGE portion contains the body of the document, which may include text, pictures, links, and/or the like).*

As to Claim 11, *Cahill anticipates method of claim 9, wherein reducing the portion of the electronic mail message comprises reducing the resolution of the at least one file associated with the electronic mail message based upon the determined file format (as stated in par. 0095, lines 1-10 the protected/encrypted content of the email is compressed to reduce the overall size thereof in existing email formats).*

As to Claim 12, *Cahill anticipates method of claim 11, wherein reducing the resolution of the at least one file comprises down casting a portion of at least one of an audio file, video file, a multimedia file, an image file, and a graphics file (as stated in par. 0067, lines 3-8, and par. 0146, lines 1-9, RM system, allows the controlled rendering of multiple forms of digital content as digital audio, digital video, digital text, digital data, and digital multimedia. The protected/encrypted content of the document is compressed to reduce the overall size thereof. Trusted component decompress the encrypted and compressed content in the course of decrypting it. Such compression provides a significant reduction in the overall size of the document having the protected content in the custom data thereof in existing document formats).*

As to Claim 13, *Cahill anticipates method of claim 1, further comprising determining that it is desirable to receive less than all of the electronic mail message (as stated in par. 0041, lines 1-13 rights management system requires only a thin client having network server interoperability and interaction. Thus, rights management system is implemented in an environment of networked hosted services in which very*

little or minimal client resources are implicated, e.g., a networked environment in which the client device serves merely as a browser or interface to receive less than all of the electronic mail message).

As to Claim 14, *Cahill anticipates method of claim 13, wherein determining that it is desirable to provide less than all of an electronic mail messages comprises (as stated in par. 0067, lines 1-9, par. 0068, lines 3-8, The main info of the email contains a message to that effect in the email, content is distributed to the user in the form of a package defining the selected format with all necessary RM-related information, rules and requirements specify and determine what to provide in e-mail to user, rules that must be satisfied before such digital content is allowed to be rendered on a user's computing device):*

determining a threshold time (as stated in par. 0071, lines 1-11, whether the user has rights to render the digital content based on any of several factors, including who the user is, where the user is located, what type of computing device the user is using, what rendering application is calling the RM system, the date, the time and limit pre-determined rendering time. Thus, the trusted component needs to refer to a clock on the computing device);

determining a value associated with a data transfer rate (as stated in par. 0072, lines 1-11 rules and requirements are specified in the license accordingly to specify attributes and values that must be satisfied which are required for the performance of functions (data transfer rate) according to specified values and attributes);

determining a value associated with a size of the electronic mail message (as stated in par. 0158, lines 1-16, RM-protected e-mail package also sets value by size of the documents by defining a specific rights template associated with the folders of digital content. Such rights template have any particular rights defined therein common to every document within the folder, or may treat different types of documents differently. The rights template for a particular folder specifies one set of rights for documents below a certain size and another set for documents above a certain size);

estimating a transfer time using the determined value associated with the data transfer rate and the determined value associated with the size of the electronic mail message (as stated in par. 0158, lines 1-10, par. 0163, lines 1-4, rights management is applied to document by way of a trusted component on a computing device of a RM-compliant recipient, and the document is in a form that is still recognizable to a computing device which may or may not be RM-compliant for receiving of protected content in such document as the protected content is rights managed, such content is compressed with value associated with the size of content document and decompressed by the trusted component of computing device based on its data transfer rate value);

comparing the threshold time and the estimated transfer time; and <u>reducing</u> a portion of the electronic mail message based upon the comparison (as stated in par. 0095, par. 0162, lines 1-4, par. 0163, lines 1-4, The protected/encrypted content 32 of the email 44 is compressed to reduce the overall size thereof. As may be appreciated, the trusted component 38 may decompress the encrypted and compressed content 32

in the course of decrypting same. As may also be appreciated, such compression provides a significant reduction in the overall size of the email 44 having the protected content 32 in the attachment 46 thereof. Notably, such compression is not presently found by default in existing email formats. Digital content are stored in the folder of the document store, the document store mapping (comparison) the access controls for the folders of digital content into RM rights that are to be defined in rights data for the copy of the requested digital content document).

As to Claim 15, *Cahill anticipates method of claim 1, wherein providing the reduced electronic mail message comprises transmitting the reduced electronic mail message from a server to a processor based device and storing the reduced electronic mail message on the server (as stated in par. 0118, lines 1-9, par. 0159-0160, to render the protected content in an RM-protected email, the protected content is encrypted according to a content key stored on RM server. Recipient of the RM-protected email must obtain a corresponding license with content key from the RM server, for obtaining protected content in the e-mail package which is stored on the RM server. In dynamically applying RM protection to a document 74 in a folder 76 in a document store 72, each document 76 is assigned a unique bind ID. Accordingly, a license 36 issued for a particular document 74 with a particular bind ID cannot be employed in connection with any other document 74 inasmuch all other documents 74 have a different bind ID. RM-protection as set for a folder 76, either by way of access controls 78 or by way of a rights template 80, may be changed from time to time by an*

administrator of the document store 72 or the like. Accordingly, it may be the case that an individual may request a document 74 from a folder 76 of the document store 72 and receive such document 74 with a first set of rights data 50, and then some time later under identical circumstances may request the same document 74 from the same folder 76 of the document store 72 and receive such document 74 with a second set of rights data 50 different from the first set).

As to Claim 16, *Cahill anticipates method of claim 1, wherein providing the reduced electronic mail message comprises transmitting the reduced electronic mail message from a processor-based device to a server and storing the reduced electronic mail message on the processor based device (as stated in par. 0121, lines 1-12, par. 0161, computing device and email application of the recipient requests the license for the protected content of the retrieved email from the RM server in a manner to satisfy the rights and conditions set forth in the license, obtains content key from the license, and applies content key to decrypt the protected content in RM-protected email. In FIG. 13, a method of using the document store 72 is shown. In such method, and as seen, the process begins by an individual storing a document 74 in a folder 76 of the document store 72 (step 1301). Presumptively, the individual storing the document 74 in the folder 76 has access rights to do so, as defined by the access controls 78 for the folder 76 or elsewhere. As was set forth above, such document as stored in the document store 72 need not be encrypted inasmuch as RM protection will be applied to a copy of the document 74 by the document store 72 when the copy is delivered to a*

requesting individual. Note again that by storing a document 74 in a particular folder 76 of the document store 72, the storing individual determines the RM-protection that is to be applied to the document 74 when retrieved from such particular folder 76 of such document store 72).

As to Claim 34, *Cahill anticipates method for interfacing with a user of a computer system having a graphical user display, comprising (as stated in par. 0049, lines 1-6, monitor or other type of display device is also connected to client computers system via an video interface or graphics interface):*

displaying at least one indicator of a digital rights management rule associated with at least one portion of at least one electronic mail message (as stated in par. 0068, lines 1-6, par. 0093, lines 1-6 The trust-based RM system allows an owner of digital content to specify license rules embodied within a digital license or use document or in the attachment of the email, and comprises several alternative forms of the body of the email, which includes user interactive text, pictures, links, metadata relating to the addenda and/or displayed on the user/user's computing device and that must be satisfied before such digital content is allowed to be rendered on a user's computing device);

monitoring the position and selection status of a pointer controller to detect that at least one of the at least one indicators has been selected by the user; and providing an indication of a user authorization associated with the at least one portion of the at least one electronic mail message and the digital rights management rule in response to

detecting that at least one of the at least one indicators has been selected by the user (as stated in par. 0068, lines 1-6, par. 0069, lines 1-10, and par. 0070, lines 1-8, Such license rules include the aforementioned requirement, that the user/user's computing device select to obtain from the content owner or an agent thereof. When user selects for such license, and satisfies rules and requirements are then provided with a trusted component mechanism that will evaluate rules and requirements with license evaluator (monitoring) and not render the digital content except according to the license rules embodied in the license associated with the digital content and obtained by the user, such as decryption key (authorization) for decrypting the digital content, and encrypted according to a key decrypt able by the user's computing device).

As to Claim 35, *Cahill anticipates method of claim 34, wherein providing the indication of the user authorization comprises providing at least one of an option to acquire one or more digital rights and an option to downcast the at least one portion of the at least one electronic mail message (as stated in par. 0077, lines 1-11, digital license rules and requirements for the email content is typically obtained from an RM server with options that such license may be sent with the email under at least some circumstances, may be obtained upon opening the email, may be obtained upon downloading the email, may be obtained at the direction of the sender and/or recipient user/user's computing device).*

As to Claim 36, *Cahill anticipates method of claim 34, further comprising providing an option to modify the digital rights management rule associated with the at least one portion of the at least one electronic mail message in response to detecting that at least one of the at least one indicators has been selected by the user (as stated in par. 0160, lines 1-11, RM-protection as set for a folders of digital content, either by way of access controls or by way of a rights template, may be changed from time to time by an administrator of the document store or the like. Accordingly, it may be the case that an email recipient user/user's may request (select) a document from a folder of the document store and receive such document with a first set of rights data, and then some time later under identical circumstances request (select) the same document from the same folder of the document store and receive such document with a second set of rights data different from the first set).*

As to Claim 37, *Cahill anticipates method of claim 34, further comprising controlling a pointer element on the graphical user display with a user pointer controller, the pointer controller having position and selection status responsive to operation by the user (as stated in par. 0048, lines 1-11, par. 0049, lines 1-4, user enters commands and information into the computer through input devices such as a keyboard and pointing device, commonly referred to as a mouse, trackball or touch pad. These and other input devices are connected to the processing unit through a user input interface that is coupled to the system bus. A monitor or other type of display device is also connected*

to the system bus via an interface, such as a video interface, which displays the position and selection status responsive to operation by the user of pointing device).

As to Claim 38, *Cahill anticipates method of claim 34, wherein displaying the at least one indicator of the indication of the user authorization associated with the at least one portion of the at least one electronic mail message and the digital rights management rule comprises displaying at least one of a closed-lock icon and an open-lock icon (as stated in par. 0078, lines 1-15, par. 0140, lines 1-11, email with the protected content may be received by an RM-compliant individual with a trusted component and the like, which is in a form amenable to such RM-compliant individual. At the same time, email with the protected content may be received by a non-RM-compliant individual without a trusted component and the like, such email should also be in a form amenable to such non-RM-compliant individual, at least to the extent that the email is recognizable as such by the computing device of the non-RM-compliant individual, informs the non-compliant individual of the protected content therein and does not inappropriately affect the computing device of the non-RM-compliant individual. Put another way, the email with the protected content is in a more-or-less standard email form so as to be recognized as email, but should also include within the standard form the protected content of the email along with all necessary RM-related information for unlocking the protected content).*

Remarks

5. The following pertaining arts are discovered and not used in this office action. Office reserves the right to use these arts in later actions.

a. Shamoon; Talal G. et al. (US 7233948 B1) Methods and apparatus for persistent control and protection of content

b. Schwartz; Bruce V. et al. (US 7003284 B2) Method and architecture for interactive two-way communication devices to interact with a network

c. Larsen; Per Buch (US 7305443 B2) System and method for tailoring of electronic messages

d. Kaghazian; Leila (US 6563913 B1) Selective sending of portions of electronic content

e. Godfrey; James A. et al. (US 7317699 B2) System and method for controlling configuration settings for mobile communication devices and services

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Muktesh G. Gupta whose telephone number is 571-270-5011. The examiner can normally be reached on Monday-Friday, 8:00 a.m. -5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William C. Vaughn can be reached on 571-272-3922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MG

/William C. Vaughn, Jr./

Supervisory Patent Examiner, Art Unit 2444